

02.02.01

JP 01/772 日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#4

EU

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

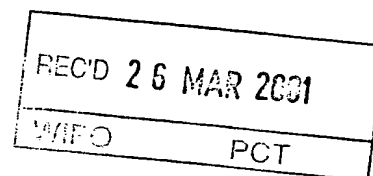
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 7月11日

出願番号
Application Number:

特願2000-209675



出願人
Applicant(s):

ソニー株式会社

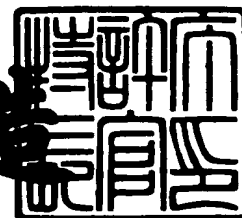
09/937797

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3015162

【書類名】 特許願

【整理番号】 0000065405

【提出日】 平成12年 7月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 金巻 裕史

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 中村 嘉秀

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 佐竹 清

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置、処理装置、認証システムおよびその方法

【特許請求の範囲】

【請求項 1】

認証要求に応じて認証処理を行う認証装置であって、
利用者を識別するための第 1 の識別情報と、前記認証要求の送信元の装置を識別する第 2 の識別情報とを含む前記認証要求を受信する受信手段と、
前記第 1 の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、
前記認証要求に応じて認証処理を行う認証処理手段と、
前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第 2 の識別情報とを対応付けて送信する送信手段と
を有する認証装置。

【請求項 2】

前記受信手段は、暗号化された前記第 1 の識別情報および前記第 2 の識別情報を含む前記認証要求を受信し、
前記認証装置は、
前記受信した認証要求に含まれる前記第 1 の識別情報および前記第 2 の識別情報を復号する復号手段
をさらに有する請求項 1 に記載の認証装置。

【請求項 3】

前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する
請求項 1 に記載の認証装置。

【請求項 4】

前記第 1 の識別情報は、登録した利用者に予め割り当てられた識別子である
請求項 1 に記載の認証装置。

【請求項 5】

前記第 2 の識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である

請求項 1 に記載の認証装置。

【請求項 6】

ネットワークを介して行われる取引に関する認証処理を行う認証装置であって、

利用者を識別するための第 1 の識別情報と、取引の内容を示す取引情報と、前記認証要求の送信元の装置を識別する第 2 の識別情報とを含み前記取引を行う利用者による前記認証要求を受信する受信手段と、

前記第 1 の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記受信した認証要求に含まれる前記取引情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、

前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第 2 の識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項 7】

前記認証処理手段は、

前記取引情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する

請求項 6 に記載の認証装置。

【請求項 8】

前記記憶手段は、

前記認証要求を発した利用者と前記指定された利用者との間の取引の履歴

情報を記憶する

請求項 6 に記載の認証装置。

【請求項 9】

前記受信手段は、暗号化された前記第 1 の識別情報および前記第 2 の識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記第 1 の識別情報および前記第 2 の識別情報を復号する復号手段

をさらに有する請求項 6 に記載の認証装置。

【請求項 10】

前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する

請求項 6 に記載の認証装置。

【請求項 11】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項 6 に記載の認証装置。

【請求項 12】

ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、

利用者を識別するための第 1 の識別情報と、当該処理装置を識別するための第 2 の識別情報とを含む前記認証要求を送信する送信手段と、

認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、

前記第 2 の識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段と

を有する処理装置。

【請求項 13】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 1 2 に記載の処理装置。

【請求項 1 4】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 2 に記載の処理装置。

【請求項 1 5】

ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、

前記認証装置は、

利用者を識別するための第 1 の識別情報と、前記認証要求の送信元の装置を識別する第 2 の識別情報とを含む前記認証要求を受信する受信手段と、

前記第 1 の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第 2 の識別情報とを含む認証応答を送信する送信手段と

を有し、

前記処理装置は、

前記第 1 の識別情報と、当該処理装置を識別するための前記第 2 の識別情報とを含む前記認証要求を送信する送信手段と、

前記認証応答を受信する受信手段と、

当該処理装置の前記第 2 の識別情報と、前記認証応答に含まれる前記第 2 の識別情報とが一致するか否かを判断する制御手段と

を有する

認証システム。

【請求項 1 6】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 1 5 に記載の認証システム。

【請求項 1 7】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 5 に記載の認証システム。

【請求項 1 8】

ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、

利用者を識別するための第 1 の識別情報と、当該処理装置を識別するための第 2 の識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、

前記認証装置において前記認証要求に応じて認証処理を行い、

前記認証装置から、前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記第 2 の識別情報とを含む認証応答を送信し、

前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記第 2 の識別情報と、当該処理装置の前記第 2 の識別情報と、前記認証応答に含まれる前記第 2 の識別情報とが一致するか否かを判断する

認証方法。

【請求項 1 9】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する

請求項 1 8 に記載の認証方法。

【請求項 2 0】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 8 に記載の認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子商取引情報を認証する認証装置、処理装置、認証システムおよびその方法に関する。

【0002】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ID情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【0003】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取り引きに関する決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する処理を行う認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【0004】

【発明が解決しようとする課題】

ところで、上述したような認証装置では、例えば、個人ID情報を他人が不正

に取得した場合に、当該他人は、その個人ID情報を用いて、認証装置に対して認証要求を出すことができ、不正な取り引きが行われてしまう可能性があるという問題がある。

【0005】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ID情報に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供することを目的とする。

【0006】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の認証装置は、認証要求に応じて認証処理を行う認証装置であって、利用者を識別するための第1の識別情報と、前記認証要求の送信元の装置を識別する第2の識別情報とを含む前記認証要求を受信する受信手段と、前記第1の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記第1の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第2の識別情報とを対応付けて送信する送信手段とを有する。

【0007】

第1の発明の認証装置の作用は以下ようになる。

例えば、利用者が端末装置などを操作して当該端末装置から送信された、利用者を識別するための第1の識別情報と、認証要求の送信元の装置を識別する第2の識別情報とを含む前記認証要求が受信手段で受信される。

次に、当該受信された前記認証要求に応じた認証処理が認証処理手段で行われる。

次に、送信手段によって、前記認証要求に含まれる前記第1の識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含ま

れる前記第 2 の識別情報とが対応付けて送信手段から送信される。

【 0 0 0 8 】

また、第 1 の発明の認識装置は、好ましくは、前記受信手段は、暗号化された前記第 1 の識別情報および前記第 2 の識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記第 1 の識別情報および前記第 2 の識別情報を復号する復号手段をさらに有する。

【 0 0 0 9 】

また、第 1 の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する。

【 0 0 1 0 】

また、第 1 の発明の認証装置は、好ましくは、前記第 1 の識別情報は、登録した利用者に予め割り当てられた識別子である。

【 0 0 1 1 】

また、第 1 の発明の認証装置は、好ましくは、前記第 2 の識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である。

【 0 0 1 2 】

第 2 の発明の認証装置は、ネットワークを介して行われる取引に関する認証処理を行う認証装置であって、利用者を識別するための第 1 の識別情報と、取引の内容を示す取引情報と、前記認証要求の送信元の装置を識別する第 2 の識別情報とを含み前記取引を行う利用者による前記認証要求を受信する受信手段と、前記第 1 の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記受信した認証要求に含まれる前記取引情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第 2 の識別情報とを対応付けて送信する送信手段とを有する。

【 0 0 1 3 】

第 2 の発明の認証装置の作用は以下になる。

利用者を識別するための第 1 の識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する第 2 の識別情報とを含み前記取り引きを行う利用者による前記認証要求が受信手段で受信される。

次に、認証処理手段によって、前記受信した認証要求に含まれる前記取り引き情報が前記認証要求によって指定された利用者の装置に送信され、当該指定された利用者の装置からの応答に応じて、所定の認証処理が行われる。

次に、送信手段によって、前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第 2 の識別情報とを対応付けて送信手段から送信される。

【 0 0 1 4 】

また、第 2 の発明の認証装置は、好ましくは、前記認証処理手段は、前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する。

【 0 0 1 5 】

また、第 2 の発明の認証装置は、好ましくは、前記記憶手段は、前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する。

【 0 0 1 6 】

また、第 2 の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記第 1 の識別情報および前記第 2 の識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記第 1 の識別情報および前記第 2 の識別情報を復号する復号手段をさらに有する。

【 0 0 1 7 】

また、第 2 の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信す

る。

【0018】

また、第2の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【0019】

また、第3の発明の処理装置は、ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、利用者を識別するための第1の識別情報と、当該処理装置を識別するための第2の識別情報とを含む前記認証要求を送信する送信手段と、認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、前記第2の識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段とを有する。

【0020】

また、第3の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する。

【0021】

また、第3の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引きの取り引き先の装置に所定の通知を行う。

【0022】

また、第4の発明の認証システムは、ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、前記認証装置は、利用者を識別するための第1の識別情報と、前記認証要求の送信元の装置を識別する第2の識別情報とを含む前記認証要求を受信する受信手段と、前記第1の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記第1の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第2の識別情報とを含む認証応答を送信する送信手段と

を有し、前記処理装置は、前記第 1 の識別情報と、当該処理装置を識別するための前記第 2 の識別情報とを含む前記認証要求を送信する送信手段と、前記認証応答を受信する受信手段と、当該処理装置の前記第 2 の識別情報と、前記認証応答に含まれる前記第 2 の識別情報とが一致するか否かを判断する制御手段とを有する。

【 0 0 2 3 】

また、第 5 の発明の認証方法は、ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、利用者を識別するための第 1 の識別情報と、当該処理装置を識別するための第 2 の識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、前記認証装置において前記認証要求に応じて認証処理を行い、前記認証装置から、前記認証要求に含まれる前記第 1 の識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記第 2 の識別情報とを含む認証応答を送信し、前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記第 2 の識別情報と、当該処理装置の前記第 2 の識別情報と、前記認証応答に含まれる前記第 2 の識別情報とが一致するか否かを判断する。

【 0 0 2 4 】

また、第 5 の発明の認証方法は、好ましくは、前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する。

【 0 0 2 5 】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図 1 は、本実施形態のトランザクション認証システム 1 0 1 の全体構成図である。

図 1 に示すように、トランザクション認証システム 1 0 1 では、例えば、発注者 3 1 の発注者端末装置 1 1 と、受注者 3 3 の受注者端末装置 1 5 と、ネットワーク銀行 4 0 の認証装置 5 0 とが、インターネットなどのネットワーク（通信網

）を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取り引き）の正当性を認証装置 5 0 で認証する。

なお、当該ネットワークに接続されている発注者端末装置 1 1 および発注者受注者端末装置 1 5 の数は任意である。

【 0 0 2 6 】

本実施形態では、発注者端末装置 1 1 が第 3 の発明の処理装置に対応し、認証装置 5 0 が本発明の認証装置に対応している。

【 0 0 2 7 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 4 0 との間で認証を行うことに関する契約が成されている。また、発注者 3 1 と引き落とし銀行 4 2 との間では、例えば、ネットワーク銀行 4 0 によって認証された取り引きに関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 4 0 と保険会社 4 3 との間では、ネットワーク銀行 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

【 0 0 2 8 】

以下、トランザクション認証システム 1 0 1 を構成する各装置について説明する。

〔発注者端末装置 1 1〕

図 2 に示すように、発注者端末装置 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 6 1、送信部 6 2、暗号化部 6 3、復号部 6 4、記憶部 6 5、制御部 6 6 および署名検証部 6 7 を有する。

なお、発注者端末装置 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な利用者であることを認証する生体認証部を有していてもよい。

【 0 0 2 9 】

ここで、受信部 6 1 が第 3 の発明の受信手段に対応し、送信部 6 2 が第 3 の発明の送信手段に対応し、制御部 6 6 が第 3 の発明の制御手段に対応している。

【0030】

受信部61は、ネットワークを介して認証装置50から情報あるいは要求を受信する。

送信部62は、ネットワークを介して認証装置50に情報あるいは要求を送信する。

また、受信部61および送信部62は、受注者33が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部63は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部64は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部65は、製造元で受注者端末装置15に付された装置ID情報 ID_M （本発明の第2の識別情報）と、発注者31が作成した秘密鍵 $K_{33,S}$ などを格納する。

署名検証部67は、例えば、認証装置50が作成した署名情報を、ネットワーク銀行40の公開鍵 $K_{40,P}$ を用いて検証する。

制御部66は、発注者端末装置11内の各構成要素の処理を統括的に制御する。

【0031】

制御部66は、例えば、発注者31による操作に応じて、発注情報 a_1 と、個人キー情報 k_1 （本発明の第1の識別情報）と、個人ID情報 ID_1 （本発明の第1の識別情報）と、記憶部65から読み出した装置ID情報 ID_M との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf_1 を生成する。

また、制御部66は、例えば、認証要求 Inf_1 を認証装置50に送信した後に、認証装置50から認証応答 Inf_4 を受信したときに、認証応答 Inf_4 に含まれる認証要求の送信元の装置を示す装置ID情報 ID_M と、記憶部65から読み出した発注者端末装置11の装置ID情報 ID_M とが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置15

および認証装置 50 の少なくとも一方に通知する。

【0032】

〔受注者端末装置 15〕

図 3 に示すように、受注者端末装置 15 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 33 が使用するサーバ装置であり、受信部 71、送信部 72、暗号化部 73、復号部 74、記憶部 75、制御部 76 および署名検証部 77 を有する。

受信部 71 は、ネットワークを介して認証装置 50 から情報あるいは要求を受信する。

送信部 72 は、ネットワークを介して認証装置 50 に情報あるいは要求を送信する。

また、受信部 71 および送信部 72 は、発注者端末装置 11 からのアクセスに応じて、例えば、記憶部 75 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 11 に送信する。

暗号化部 73 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 74 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 75 は、受注者 33 が作成した秘密鍵 $K_{33,S}$ などを格納する。

制御部 76 は、受注者端末装置 15 内の各構成要素の処理を統括的に制御する。

署名検証部 77 は、例えば、ネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて、認証装置 50 が作成した署名情報の検証を行う。

【0033】

〔認証装置 50〕

図 4 に示すように、認証装置 50 は、受信部 81、送信部 82、暗号化部 83、復号部 84、記憶部 85、制御部 86、署名作成部 87 および課金処理部 88 を有する。

【0034】

ここで、受信部 81 が第 1 および第 2 の発明の受信手段に対応し、送信部 82 が第 1 および第 2 の発明の送信手段に対応し、記憶部 85 が第 1 および第 2 の発

明の記憶手段に対応し、制御部 86 が第 1 および第 2 の発明の認証処理手段に対応している。

【0035】

受信部 81 は、ネットワークを介して発注者端末装置 11 および受注者端末装置 15 から情報あるいは要求を受信する。

送信部 82 は、ネットワークを介して発注者端末装置 11 および受注者端末装置 15 に情報あるいは要求を送信する。

暗号化部 83 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 84 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 85 は、発注者 31 がネットワーク銀行 40 と契約したときに、発注者 31 の個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者端末装置 11 のアドレス（または、発注者端末装置 11 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を記憶する。また、記憶部 85 は、例えば、発注者 31 および受注者 33 がネットワーク銀行 40 と契約をしたときに、発注者 31 が作成した秘密鍵 $K_{31,S}$ に対応する公開鍵 $K_{31,P}$ 、並びに受注者 33 が作成した秘密鍵 $K_{33,S}$ に対応する公開鍵 $K_{33,P}$ などを格納する。

制御部 86 は、認証装置 50 内の各構成要素の処理を統括的に制御する。

署名作成部 87 は、ネットワーク銀行 40 の秘密鍵 $K_{40,S}$ を用いて署名情報の作成を行う。

課金処理部 88 は、発注者 31 による取引に関する認証に対しての課金処理を行う。

認証装置 50 の各構成要素の詳細な処理については、後述する動作例で記載する。

【0036】

以下、トランザクション認証システム 101 の動作例を説明する。

当該動作例を開始する前提として、発注者 31 とネットワーク銀行 40 との間で所定の契約が結ばれ、ネットワーク銀行 40 は、発注者 31 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行する。

ネットワーク銀行 40 は、個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注

者端末装置 11 のアドレス（または、発注者端末装置 11 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を図 4 に示す認証装置 50 の記憶部 85 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 40 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

【0037】

また、ネットワーク銀行 40 は、自らの秘密鍵 $K_{40,S}$ を図 4 に示す認証装置 50 の記憶部 85 に記憶すると共に、当該秘密鍵 $K_{40,S}$ に対応する公開鍵 $K_{40,P}$ を発注者端末装置 11 および受注者端末装置 15 に送信する。発注者端末装置 11 は、公開鍵 $K_{40,P}$ を図 2 に示す記憶部 65 に記憶する。受注者端末装置 15 は、公開鍵 $K_{40,P}$ を図 3 に示す記憶部 75 に記憶する。

【0038】

また、受注者 33 とネットワーク銀行 40 との間で所定の契約が結ばれ、ネットワーク銀行 40 は、受注者 33 に対して、個人キー情報 Z および個人 ID 情報 ID_2 を発行する。ネットワーク銀行 40 は、個人キー情報 Z および個人 ID 情報 ID_2 の対応表を図 4 に示す認証装置 50 の記憶部 85 に記憶する。

【0039】

図 5 は、トランザクション認証システム 101 の動作例を説明するための図である。

ステップ ST11 :

図 1 に示す発注者 31 は、例えばネットワーク上の商店である受注者 33 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a_1 と、発注者 31 の個人キー情報 k_1 と、発注者 31 の個人 ID 情報 ID_1 とを、図示しない操作手段を操作して発注者端末装置 11 に入力する。なお、発注情報 a_1 には、受注者 33 を特定する情報が含まれている。

次に、図 2 に示す発注者端末装置 11 の暗号化部 63 は、記憶部 65 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて、発注情報 a_1 と、個人キー情報 k_1 と、個人 ID 情報 ID_1 と、記憶部 65 から読み出した装置 ID 情報

ID_M との全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求 $Inf1$ (本発明の第1の要求) を、送信部62からネットワークを介して、図1に示すネットワーク銀行40の認証装置50に送信する。

【0040】

ステップST12:

図4に示す認証装置50は、発注者端末装置11からの認証要求 $Inf1$ を受信部81が受信すると、記憶部85からネットワーク銀行40の秘密鍵 $K_{40,S}$ を読み出し、復号部84において、当該秘密鍵 $K_{40,S}$ を用いて認証要求 $Inf1$ を復号する。

次に、認証装置50は、制御部86の制御に基づいて、上記復号した認証要求 $Inf1$ に格納された発注情報 $a1$ および個人キー情報 $k1$ を格納した情報 $Inf1'$ について、記憶部85から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報 $Au1$ を作成する。

次に、認証装置50は、情報 $Inf1'$ および署名情報 $Au1$ を格納した要求 $Inf2$ を生成する。

次に、暗号化部83は、図4に示す記憶部85から読み出した受注者33の公開鍵 $K_{33,P}$ を用いて、上記生成した要求 $Inf2$ を暗号化した後に、送信部82から、ネットワークを介して受注者端末装置15に送信する。

【0041】

ステップST13:

受注者端末装置15の復号部74は、認証装置50からの要求 $Inf2$ を受信部71が受信すると、記憶部75から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求 $Inf2$ を復号する。

次に、受注者端末装置15の署名検証部77は、上記復号した要求 $Inf2$ に格納された署名情報 $Au1$ を、記憶部75から読み出した認証装置50の公開鍵 $K_{40,P}$ を用いて検証する。

【0042】

受注者端末装置15の制御部76は、署名検証部が上記検証の結果、署名情報 $Au1$ の正当性が認証されると、要求 $Inf2$ に格納された情報 $Inf1'$ を図

3に示す記憶部75に記憶する。受注者33は、情報Inf1'内の発注情報a1に基づいて、発注者31への商品等の発送予定などを示す受注確認情報c1を生成する。

次に、制御部76は、要求Inf2、受注確認情報c1および自らの個人情報Zを格納した応答Inf3を生成する。

次に、受注者端末装置15の送信部72は、上記生成した応答Inf3を、記憶部75から読み出したネットワーク銀行40の公開鍵 $K_{40,P}$ を用いて暗号化部73で暗号化した後に、送信部72から、ネットワークを介して認証装置50に送信する。

受注者33は、例えば、要求Inf2に格納された情報Inf1'内の発注情報a1に基づいて、発注者31が発注した商品等を発注者31に発送したり、発注者31が注文したサービスを発注者31に提供する。

【0043】

ステップST14:

認証装置50の復号部84は、受注者端末装置15からの応答Inf3を受信部81が受信すると、記憶部85から読み出した自らの秘密鍵 $K_{40,S}$ を用いて、Inf3を復号し、要求Inf1に格納された発注情報a1と、当該復号されたInf3に格納された受注者33の個人情報Zとを用いて、所定の取り引き履歴情報を作成し、これを記憶部85に格納する。当該履歴情報は、ネットワーク銀行40が、発注者31に対して決済を行う際に用いられる。

また、認証装置50の署名作成部87は、ステップST13で受信した応答Inf3について、自らの秘密鍵 $K_{40,S}$ を用いて署名情報Au2を作成する。

次に、認証装置50の制御部86は、応答Inf3および署名情報Au2を格納した認証応答Inf4を作成する。

次に、認証装置50の暗号化部83は、上記作成し認証した応答Inf4を、記憶部85から読み出した発注者31の公開鍵 $K_{31,P}$ を用いて暗号化した後に、送信部82から、ネットワークを介して発注者端末装置11に送信する。

【0044】

ステップST15:

発注者端末装置 11 では、受信した認証応答 Inf 4 を、図 2 示す記憶部 65 から読み出した発注者 31 の秘密鍵 $K_{31,S}$ を用いて復号部 64 で復号する。

次に、発注者端末装置 11 の署名検証部 66 は、当該復号した認証応答 Inf 4 に格納された署名情報 Au 2 を、記憶部 65 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて検証すると共に、Inf 4 内の発注情報 a 1 内に記述された装置 ID 情報 ID_M が図 2 に示す発注者端末装置 11 の記憶部 65 に記憶されている自らの装置 ID 情報 ID_M と一致するかを判断し、一致すると判断した場合には、受注者 33 との間の当該取り引きが正当に行われたことを確認する。発注者端末装置 11 は、Inf 4 内の発注情報 a 1 内に記述された装置 ID 情報 ID_M が図 2 に示す発注者端末装置 11 の記憶部 65 に記憶されている自らの装置 ID 情報 ID_M と一致しないと判断した場合には、例えば、認証応答 Inf 4 を格納した不正発注通知 Inf 5 を認証装置 50 および受注者端末装置 15 の少なくとも一方に送信する。

これにより、認証装置 50 および受注者端末装置 15 は、発注者端末装置 11 が発した認証要求 Inf 1 に対応した発注を取り消す。

また、発注者端末装置 11 は、不正発生通知 Inf 5 を、図 1 に示す引き落とし銀行 42 に送信してもよい。

【0045】

以上説明したように、トランザクション認証システム 101 によれば、認証要求 Inf 1 内に、個人 ID 情報 ID 1 の他に当該認証要求を出した装置 ID 情報 ID_M を自動的に挿入し、認証装置 50 において、認証要求 Inf 1 に含まれる発注者 31 が使用する発注者端末装置 11 のアドレスに、認証結果を含む認証応答 Inf 4 を送信し、当該認証応答 Inf 4 内に当該認証要求を出した装置 ID 情報 ID_M を格納することで、発注者端末装置 11 では、認証応答 Inf 4 に格納された当該認証要求を出した装置 ID 情報 ID_M と自らの装置 ID 情報 ID_M とが一致するか否かを判断することで、自らの個人 ID 情報 ID 1 を用いた不正な認証要求（なりすまし）が発生したことを検出できる。

その結果、トランザクション認証システム 101 によれば、他人の個人 ID 情報を用いた不正な取り引きを効果的に抑制できる。

【0046】

上述したように、トランザクション認証システム101によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取引引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【0047】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、発注者端末装置11において、認証応答Inf4内の発注情報a1内に記述された装置ID情報ID_Mが図2に示す発注者端末装置11の記憶部65に記憶されている自らの装置ID情報ID_Mと一致するかを判断し、一致しないと判断した場合には、例えば、認証応答Inf4を格納した不正発注通知Inf5を認証装置50および受注者端末装置15の少なくとも一方に送信する場合を例示したが、例えば、一致しない旨（不正な取引引きが行われた旨）を発注者端末装置11のディスプレイなどに表示し、発注者31にその旨を知らせるようにしてもよい。

また、発注者端末装置11において、上述した装置ID情報ID_Mの一致を判断するのではなく、発注者31が判断してもよい。

また、発注者端末装置11が配設された家庭にホーム・ゲートウェイ(Home Gateway)が設置されている場合には、ホーム・ゲートウェイに発注者端末装置11の装置ID情報ID_Mを登録しておき、認証装置50からの認証応答Inf4をホーム・ゲートウェイが受信したときに、ホーム・ゲートウェイにおいて、上記装置ID情報ID_Mの一致の判断を行ってもよい。

【0048】

また、上述した実施形態では、ネットワーク銀行40が、認証装置50を用いて、トランザクション（取引引き）の認証業務を行う場合を例示したが、ネットワーク銀行40とは別の機関が、認証装置50を用いてトランザクションの認証業務を行うようにしてもよい。

【0049】

また、上述した実施形態では、図5に示すステップST11のように、暗号化

された発注情報 a 1 と、個人キー情報 k 1 と、個人 I D 情報 I D 1 と、装置 I D 情報 I D_M とを含む認証要求 I n f 1 を、発注者端末装置 1 1 から認証装置 5 0 に送信する場合を例示したが、発注情報 a 1 と、個人キー情報 k 1 と、装置 I D 情報 I D_M とを含む認証要求 I n f 1 を、発注者端末装置 1 1 から認証装置 5 0 に送信してもよい。このようにすれば、課金に係わる情報である個人 I D 情報 I D 1 はネットワークを介して伝送されないため、ネットワーク上で個人 I D 情報 I D 1 が不正に取得され、悪用されることを回避できる。

【 0 0 5 0 】

また、上述した実施形態では、図 2 に示す発注者端末装置 1 1 の暗号化部 6 3 において、記憶部 6 5 から読み出した所定の暗号鍵を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 I D 情報 I D 1 と、記憶部 6 5 から読み出した装置 I D 情報 I D_M との全体に対して暗号化を行う場合を例示したが、発注情報 a 1 と、個人キー情報 k 1 と、個人 I D 情報 I D 1 と、記憶部 6 5 から読み出した装置 I D 情報 I D_M とのそれぞれについて個別に暗号化を行ってもよい。

【 0 0 5 1 】

【発明の効果】

以上説明したように、本発明によれば、不正に取得した他人の識別情報（個人 I D 情報）に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供できる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図 2】

図 2 は、図 1 に示す発注者端末装置の構成図である。

【図 3】

図 3 は、図 1 に示す受注者端末装置の構成図である。

【図 4】

図 4 は、図 1 に示す認証装置の構成図である。

【図 5】

図 5 は、図 1 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【符号の説明】

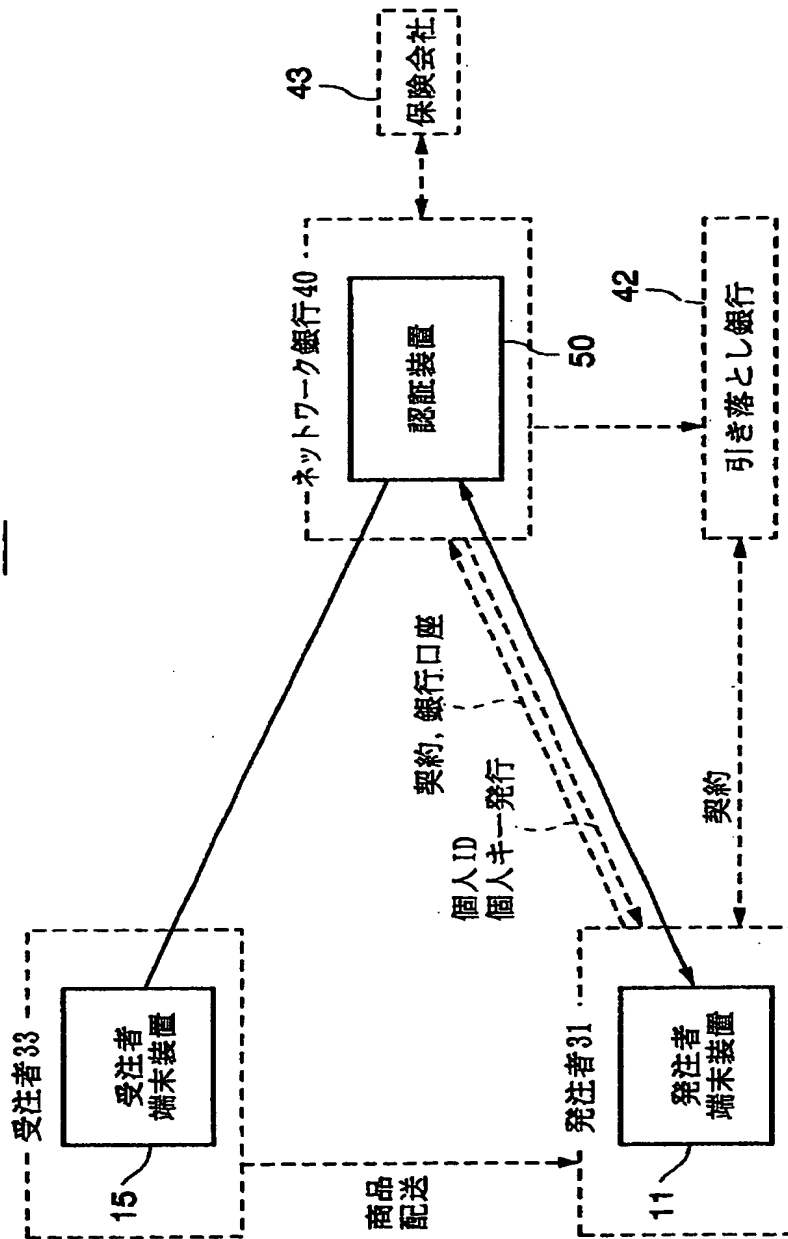
1 … トランザクション認証システム、11 … 発注者端末装置、15 … 受注者端末装置、31 … 発注者、33 … 受注者、40 … ネットワーク銀行、50 … 認証装置、61, 71, 81 … 受信部、62, 72, 82 … 送信部、63, 73, 83 … 暗号化部、64, 74, 84 … 復号部、65, 75, 85 … 記憶部、66, 76, 86 … 制御部、67, 77 … 署名検証部、87 … 署名作成部、88 … 課金処理部、a1 … 発注情報、k1 … 発注者 31 の個人キー情報 k1、ID1 … 発注者 31 の個人 ID 情報、ID_M … 装置 ID 情報、Au1, Au2 … 認証装置の署名情報、Z … 受注者の個人キー情報、Inf1 … 認証要求、Inf4 … 認証応答

【書類名】

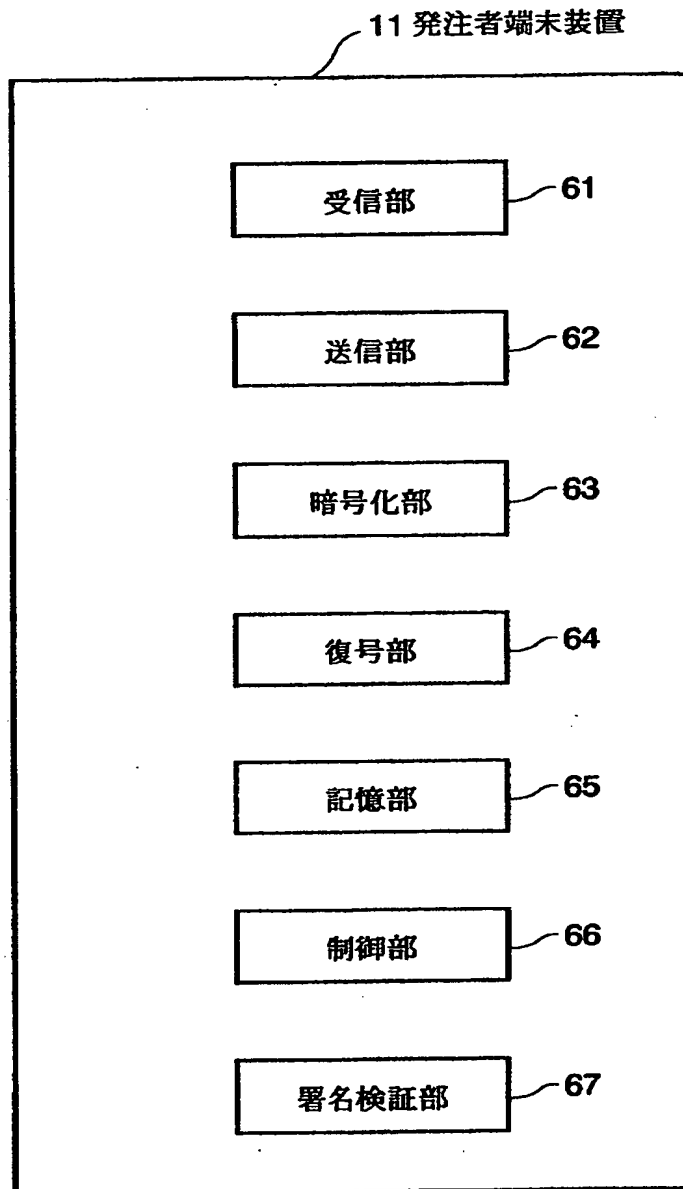
図面

【図 1】

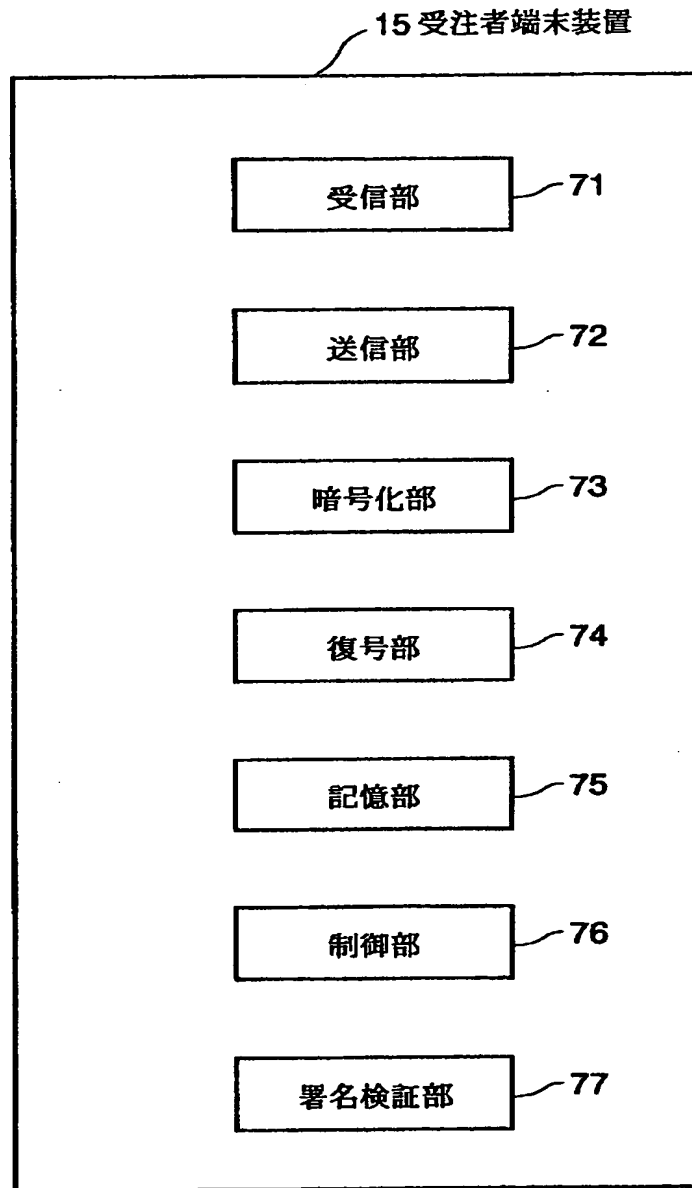
101



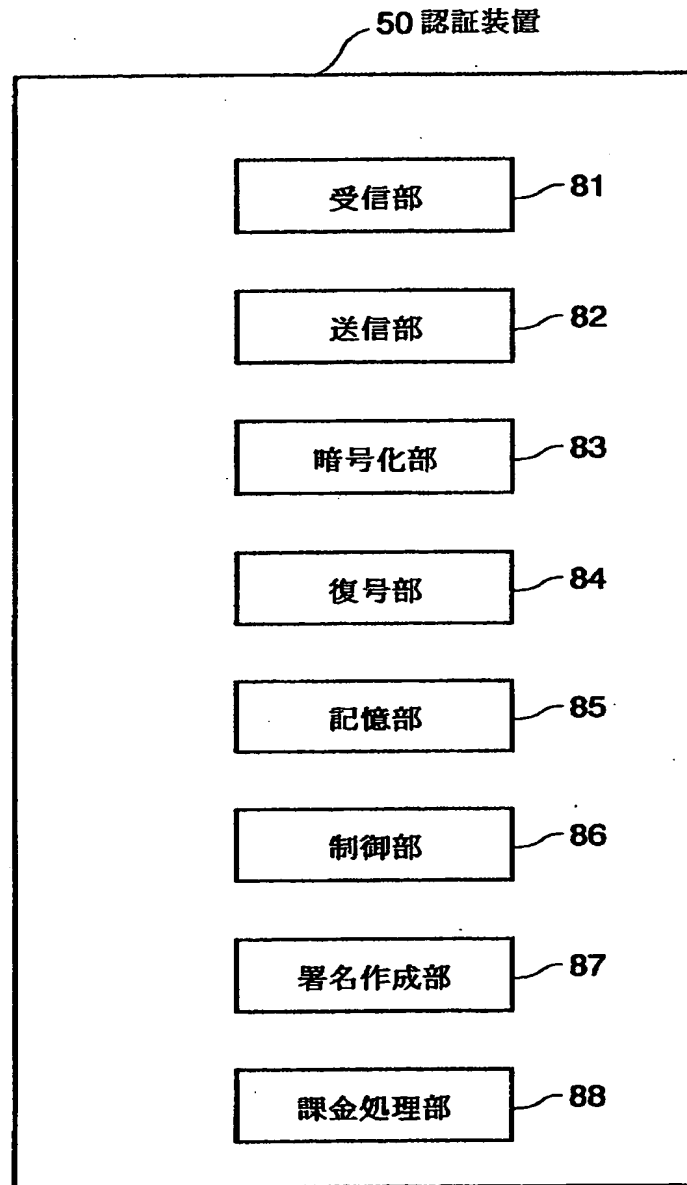
【図 2】



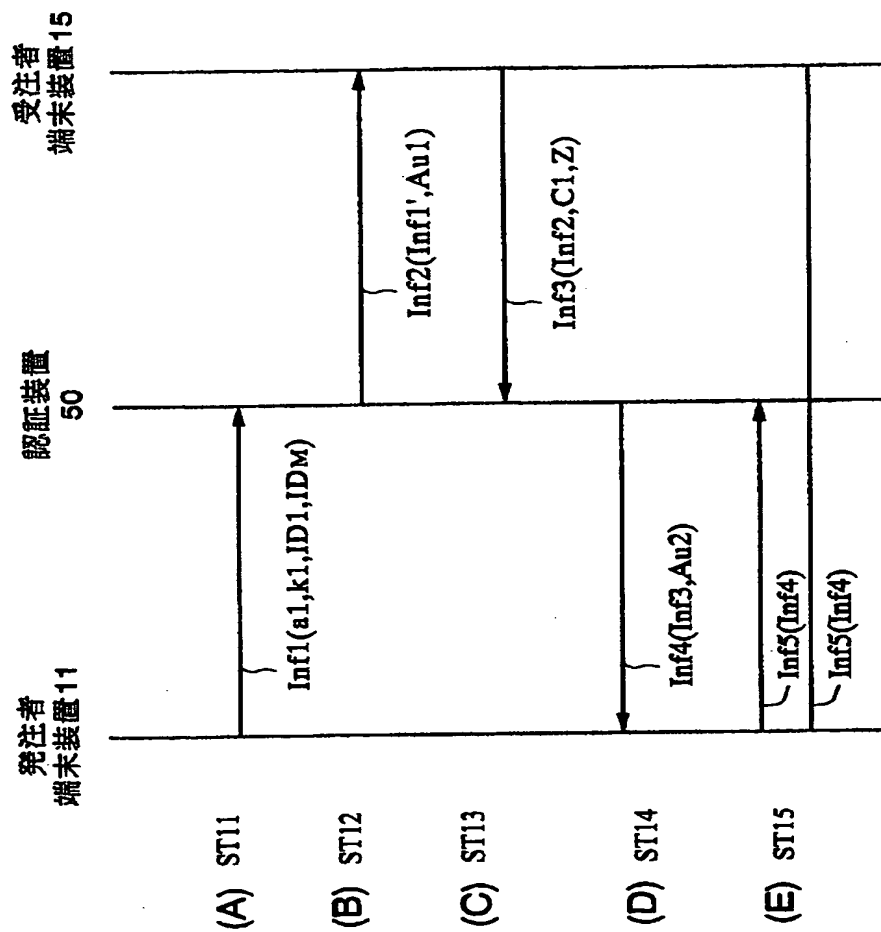
【図 3】



【図4】



【図 5】



【書類名】 要約書

【要約】

【課題】 不正に取得した他人の個人ID情報に基づいて不正な認証手続きが行われることを回避する認証装置を提供する。

【解決手段】 認証装置50は、発注者端末装置11からの認証要求によって、発注者端末装置11を特定する装置ID情報ID_Mと、発注者31を特定する個人ID情報等を受信し、受注者端末装置15との間の通信を行った後に、認証要求に含まれた装置ID情報ID_Mを含む認証応答を発注者端末装置11に送信する。発注者端末装置11では、当該認証応答に含まれた装置ID情報ID_Mが自らの装置ID情報ID_Mと一致するかを確認する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社